(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 March 2001 (22.03.2001)

PCT

(10) International Publication Number
WO 01/20829 A1

(51) International Patent Classification[7]: H04J 3/14, H04L 1/22, 12/26

(21) International Application Number: PCT/US00/23498

(22) International Filing Date: 28 August 2000 (28.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/395,831 14 September 1999 (14.09.1999) US

(71) Applicant: MEGAXESS, INC. [US/US]; Trevion II, Suite 206, 12800 Middlebrook Road, Germantown, MD 20874 (US).

(72) Inventors: NEMES, Mihnea, C.; Apartment 180, 18510 Boysenberry Drive, Gaithersburg, MD 20879 (US). VAMAN, Dhadesugoor, R.; 8399 Buckeye Court, Frederick, MD 21702 (US). KIM, Dongsoo, S.; 1641 E. Jefferson Street, T3, Rockville, MD 20852 (US).

(74) Agent: FRISCIA, Michael, R.; Wolff & Samson, 5 Becker Farm Road, Roseland, NJ 07068-1776 (US).

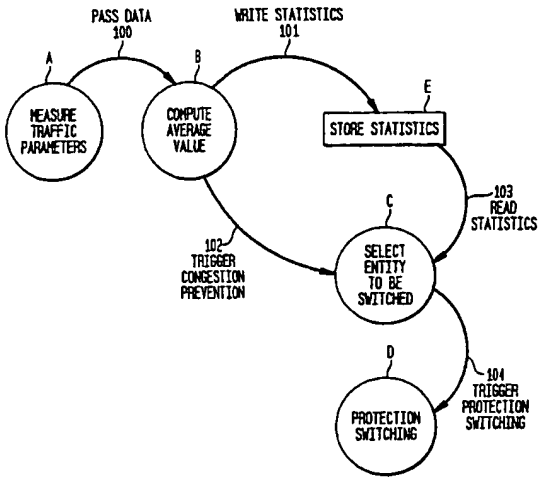
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR PREVENTION OF CONGESTION IN ATM NETWORKS THROUGH ATM PROTECTION SWITCHING



(57) Abstract: The present invention provides a method and apparatus for preventing congestion from occurring in ATM networks by treating congestion as a soft network failure and taking preventive measures before congestion occurs to prevent service degradation and insure that quality of service is provided even when traffic grows beyond an acceptable limit on a particular route. The invention uses closed loop and open loop methods for congestion control and utilizes protection switching mechanisms before congestion occurs. The present invention monitors congestion based on traffic parameter monitoring (100), average parameter values computation (101), appropriate threshold setting and selective protective switching (104). When growth of traffic threatens the quality of service in particular segment of the network, protection switching is executed selectively to divert a fraction of the traffic to relieve the traffic on the affected route.

WO 01/20829 A1

METHOD AND APPARATUS FOR PREVENTION OF CONGESTION IN ATM NETWORKS THROUGH ATM PROTECTION SWITCHING

SPECIFICATION

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention generally relates to an automatic protection switching method for preventing congestion in an ATM network, and more particularly to a method that uses ATM protection switching to prevent congestion occurrence in ATM networks by treating the onset of congestion as network soft failures.

RELATED ART

ATM network congestion control methods address the capacity of a network as a whole to carry the offered traffic. In contrast, flow control methods address the point to point communication between a sender and a receiver, by adapting the data rate of the sender to the data rate at which the receiver can process the traffic. Basically, congestion control methods addresses the ability of a network to handle traffic, while flow control addresses the ability of the receiving devices to follow the speed of the transmitting devices.

The majority of congestion control methods have traditionally been categorized as part of traffic management. Therefore, congestion control methods used in the past have involved methods that rely on modifying or shaping the traffic at the traffic source, or at the network entrance point, in order to prevent or to handle congestion. Typical congestion control techniques include "open loop" and "closed loop" methods.

Open loop methods are, by definition, measures that the network takes prior to servicing the traffic. These measures include decision mechanisms to accept or reject new traffic (Call Admission Control). These mechanisms rely on analyzing the network condition for a determined destination at the point of entrance in the network. Whenever a call setup request arrives at the network entrance point, the parameters specified in the call traffic contract are checked against the resource

based on the traffic contracts of the accepted calls in the network. These open loop methods also include packet or cell discarding or tagging. If a traffic source does not conform to the traffic contract, the packets or cells belonging to that call are discarded, or if their priority is high, the cells are tagged and their priority is changed to a lower one. Open loop methods also include traffic shaping techniques (Leaky Bucket, Token Bucket) that transform bursty traffic patterns into uniform traffic patterns. Networks that transport bursty traffic are difficult to dimension, and therefore they are subject to experience congestion. If the traffic pattern is uniform, then the network can be dimensioned so that the risk of congestion diminishes. Open loop methods are based on pre-dimensioning the network, and do not follow the dynamic changes in the network.

Closed loop methods are based on feedback received from the network. Closed loop techniques monitor the system to detect the time and location of congestion occurrence, convey the congestion notification to the parts of the system that can adjust the system operation, and ultimately, adjust the system operation. They include techniques that rely on notifying the congestion to the traffic source, which has to reduce the transmission rate for the congestion to be relieved (Source Rate Adaptation). Also included in closed loop methods are admission controls, which may be used in response to a state of network congestion, and which prevents any call from being accepted after the congested state is declared. Another closed loop method employs the use of additional bandwidth for new calls. This technique gives the possibility to offer additional bandwidth for the new calls that arrive at a congested point. This technique however, does not improve the state of the calls that are already routed through a congested path. Closed loop methods are reactive in the sense that they do not act until congestion is already in place, and therefore service degradations may occur.

Other efforts to reduce congestion and/or to overcome hard or soft network failures include:

ITU-T Recommendation I.630. The Recommendation I.630 presents the architecture and protocol related to ATM layer protection switching. It recommends that ATM protection switching be used if failures or signal degradations are detected.

"Transparent Non-disruptible ATM Network," Vaman, et al., U.S. Patent Application Serial No. 08/862,631, filed May 23, 1997, now _____, which discloses a method to provide non-disrupted service through rerouting in case of resource failure or in the case that a resource becomes unreachable (in mobile networks). Also, the invention specifies that an alarm indication management cell is used to notify about congestion. However, there is no disclosure of use of protection switching or re-routing to relieve or prevent congestion.

"Hitless ATM Cell Transport for Reliable Multi-service Provisioning" Vaman, et al., U.S. Patent Serial No. 09/249,001, filed February 12, 1999, now _____, which discloses a means of lossless conveyance of user information even when network failures occur. This method can be coupled with the invention disclosed in the present document to ensure QoS at all times.

"A Taxonomy for Congestion Control Algorithms in Packet Switching Networks", Yang C.-Q., Reddy A.V.S., IEEE Network Magazine, vol 9, pp34-35, July/Aug. 1995. In this article, a taxonomy for congestion control algorithms is given. This taxonomy is used to identify the novel features of the present disclosed congestion control method. Additionally, terminology used herein is generally defined in an ATM Forum Specification: "Traffic Management Specification Version 4.0," The ATM Forum Technical Committee, April, 1996.

In contrast with the techniques previously set forth, the present invention specifically addresses the need for preventing congestion by treating the onset of congestion as a soft-failure of a network entity. There is a need to prevent congestion before it happens through feedback from the network entity. The present invention combines the advantages of congestion prevention with the effectiveness of feedback loops.

OBJECTS AND SUMMARY OF THE INVENTION

It is a primary object of the present invention to prevent network congestion from occurring in ATM networks.

It is another object of the present invention to prevent congestion from occurring in ATM networks by treating the onset of congestion as a soft network failure.

It is an additional object of the present invention to use open loop and closed loop methods, in combination, to prevent congestion in ATM networks.

It is even an additional object of the present invention to prevent congestion from occurring in an ATM network by utilizing protection switching before congestion occurs to prevent service degregation, and to insure quality of service even when traffic grows beyond an acceptable limit on a particular route.

It is still another object of the present invention to prevent congestion from occurring by taking action at a switch in a network.

It is yet another object of the present invention to prevent congestion from occurring in an ATM network by taking advantage of network resources and finding capacity without reducing offering and without source requirements.

It is a further object of the present invention to prevent congestion from occurring in ATM networks by taking action prior to the occurrence of congestion.

It is yet an additional object of the present invention to insure quality of service (QoS) in the network, i.e. guarantee that the user sends at the same rate.

The present invention provides a method and apparatus for preventing congestion from occurring in ATM networks by treating congestion as a soft network failure and taking preventative measures before congestion occurs to prevent service degregation and insure that quality of service is provided even when traffic grows beyond an acceptable limit on a particular route. The invention uses closed loop and open loop methods for congestion control and utilizes protection switching mechanisms before congestion occurs. The present invention monitors congestion based on traffic parameter monitoring, average parameter values computation, appropriate threshold setting and selective protective switching. When growth of traffic threatens the quality of service in particular segment of the network, protection

on the affected route. The fraction of traffic that is switched can be a virtual path, a group of virtual paths, or several virtual path groups. The method comprises the steps of monitoring traffic parameters; computing the average growth of the traffic; comparing the average traffic growth with predetermined thresholds; executing selective protection switching processes when the average traffic growth exceed predetermined thresholds; executing selective protection switching by selecting the traffic fraction to be switched and switching the selected traffic fraction; monitoring the traffic parameters; and optionally returning to the original configuration if the traffic parameters return to normal values for a selected time. This process can be implemented on a microprocessor or microcontroller platform with access to the traffic parameters, and with communication access to the switching fabric. The process can be implemented in both hardware and software to be placed in existing and evolving network entities, or the apparatus can be a stand alone apparatus. The elements of the apparatus include buffer management; network management; dynamic diversion of traffic; and integration to hitless, link and hard-node failure.

BRIEF DESCRIPTION OF THE DRAWINGS

Other important objects and features of the invention will be apparent from the following Detailed Description of the Invention taken in connection with the accompanying drawings in which:

FIG. 1a is a graph of the instantaneous traffic load on the working path and **FIG 1b** is a graph of the instantaneous traffic load on the protection path.

FIG. 2 is a graph of the behavior of a network where no congestion control methods are applied.

FIG. 3 is a graph of the behavior of a network that, upon congestion, stops accepting new calls.

FIG. 4 is a graph of the behavior of a network where additional capacity is provided when congestion becomes important.

FIG. 5 is a graph of the behavior of a network that implements the method of the present invention.

FIG. 6 is a flow chart of the steps comprising the method of the present invention.

FIG. 7 is a flow chart of the step of selecting an entity to be switched.

FIG. 8 is a flow chart of the steps involved in the function of selection of **FIG. 7**.

FIG. 9a and **9b** show link utilization in a network before and after protection switching, respectively.

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to a method for preventing congestion from occurring in ATM networks. This ensures that Quality of Service (QoS) is provided even when the traffic grows beyond an acceptable limit on a particular route. QoS means that a user can send information over the network at a set rate that does not change. Moreover, when protection switching according to the present invention is executed before the congestion occurs, all the measures are preventive and therefore, service degradation is prevented. The invention can be used in connection with IP, DWDM, Wireless and DSL networks.

The method of the present invention is based on traffic parameter monitoring, average parameter values computation, appropriate threshold setting, and selective protection switching. When growth of traffic threatens the assured QoS in a particular segment of the network, protection switching is executed selectively (i.e. just a fraction of the traffic is switched) to relieve the traffic on the affected routes. The switched traffic is accommodated on pre-assigned protection paths that carry low priority (excess) traffic. The fraction of the traffic that is switched can be a Virtual Path (VP), group of Virtual Paths or Virtual Path Group (VPG), or several Virtual Path Groups (VPGs).

The present invention is based on automated protection switching at the ATM layer. Protection switching is a process where an alternate path (protection path) is provided in addition to the path in use, whenever an impairment is detected on the path is use (working path). The invention treats the onset of congestion in a network as a soft failure of the network entity where it occurs. Thus, hard failures and soft failures can be treated in an integrated manner. However, there are differences in the way soft failures (and in this case the onset of congestion) and hard failures are addressed. In order to efficiently react to a hard failure, all the traffic that was carried on the affected path must be switched onto the protection path. In the case of congestion, there is no need to switch all the traffic on the protection path, but rather only a fraction of it. This ensures that the risk of congestion on the working path is eliminated, without reducing the source information rate and without dropping cells. Since the traffic can be grouped in VCs, VPs, and even VPGs, the fraction that can

used for low priority traffic, and a spare capacity can always be reserved. The protection switching should occur only if the traffic switched would not overload or congest the protection path.

FIGS. 1a and **b** illustrates how protection switching relieves the working path by switching a fraction of the carried traffic onto the protection path. **FIG. 1a** shows the instantaneous traffic on the working path, while **FIG. 1b** shows the instantaneous traffic on the protection path. The following conventions apply:

201: Safety threshold

202: Congestion onset threshold

404: Maximum spare capacity reserved for protection switching

A, B, C: Periods in time

t0, t1: moments in time.

FIG. 1a, period A: the traffic on the working path is above the safety threshold, but no actions are taken yet. At t0, the traffic is crossing the congestion onset threshold. This starts the hold off timer. The entire period B coincides with the hold off time. At t1, since the traffic is still above the congestion onset threshold and thus the risk of congestion is high, protection switching is required. After selecting which fraction of the traffic will be switched to the protection path, the protection switching occurs. The goal is to bring the traffic on the working path below the safety threshold. At the same instance of time the traffic on the protection path increases with the amount of traffic switched from the working path. During this time no new calls are accepted on the working path.

FIGS. 2 - 4 depict the relationship between the traffic that enters in the network and the traffic that is delivered by the network for each technique presented. The following conventions are used:

201: Safety threshold

202: Congestion onset threshold

301: Maximum capacity on the working path

302: Cumulated maximum capacity on the working and protection path

A, B, C, D: Graph segments

FIG. 2 shows the behavior of a network where no congestion control

without any problems. As the traffic load approaches the maximum capacity of the network, even as the number of packets is increasing, the number of delivered packets remains the same. This is evident in Region B. However, if the number of incoming packets is increasing still, then the network will be unable to process them and as a result, many packets will be lost and not delivered. This corresponds to the congested state and to Region C, where in this case the curve reaches far.

FIG. 3 shows the behavior of a network that upon congestion stops accepting new calls. Since the number of incoming packets in this case is bounded, the congestion does not become any worse, and therefore the curve does no go far in the congested state, which is represented by Region C.

FIG. 4 show the behavior of a network where additional capacity is provided when congestion becomes important. Regions A, B, and C are the same as in **FIG. 2**. While Curve 1 and Regions A, B, and C correspond to the operation of the system at normal capacity, Curve 2 and Region D correspond to the operation of the system with additional capacity. As **FIG. 4** shows, the additional capacity is only offered after congestion has reached alarming proportions. Region D corresponds to a betterment of the network performance.

FIG. 5 shows the behavior of a network that implements the present invention. Curve 1 corresponds to the operation of the network when only the working path is used. When the traffic goes beyond the onset of congestion threshold for a period longer than the hold-off time, protection switching is executed and the traffic on the working path falls below the safety threshold. Curve 2 corresponds with the operation of the system when both working and protection paths are used. The boundary between Curve 1 and Curve 2 will fall statistically between thresholds 201 and 202. Region A, which corresponds with the optimal performance of the network, is larger than in all other cases presented, and it allows for a better packets delivered / incoming packets ratio when the number of incoming packets is larger. Limitation of the number of packets delivered occurs only at large numbers of incoming packets (Region B). Statistically, the traffic load on both paths does not go beyond the acceptable level, which assures the maintenance of QoS.

The novel features of the invention include: i. Use of a closed loop

following techniques, at the same time, to prevent congestion: increase of resources, and decrease of load on the affected route; and use of protection switching as a mechanism to prevent the occurrence of congestion. Existing closed loop congestion control methods are reactive. The mechanisms are triggered after congestion has occurred. The present invention triggers the protection switching mechanisms before congestion has occurred.

In existing congestion control algorithms, either of the two techniques is used. The present invention uses both techniques at the same time, since by executing protection switching, more bandwidth becomes available to the service, and the load is also reduced on the affected route. This ensures the Service Level Agreement (SLA) maintenance on the affected route without dropping or reducing user traffic.

The protection switching is used against node or link failures. By extending its usage to congestion prevention and congestion relieving, failures and congestion can be treated in an integrated manner.

The method of the present invention comprises the following steps: monitoring traffic parameters; computing the average growth of the traffic; comparing the average traffic growth with pre-determined thresholds; executing selective protection switching processes when the average traffic growth exceeds pre-determined thresholds; executing selective protection switching by selecting the traffic fraction to be switched and switching the selected traffic fraction; monitoring the traffic parameters and optionally returning to the original configuration if the traffic parameters return to normal values for a selected time period.

FIG. 6 shows the four steps or processes that are involved in the congestion prevention method of the present invention and the relationships among the steps. The following conventions are used:

A,B,C,D - Processes;

E - Memory shared by Processes B and C; and

100, 101, 102, 103, 104 - Interactions between processes or read/write actions from/to the shared memory.

Process "A" samples continuously the values of the traffic parameters that were chosen as a measure of congestion. Periodically, these values are passed to

"B" writes periodically the statistics to the Shared Memory "E." Also, if the parameters reach an alarm threshold, congestion prevention is triggered by launching Process "C." Process "C" selects a fraction of the traffic to be switched on the protection path, in order to relieve the working path. Process "C" may select a VC, a VP or group of VPs, depending on whether protection switching is executed at the VC, VP or VPG level. For example, if protection switching should be executed at the VPG level, the output of the selection process will indicate which VPG must be switched in order to relieve the working path. In this case, the selected entity is a VPG. Once an entity has selected, Process "D," Protection Switching, is launched for that entity.

Process "A," which relates to the traffic parameters measurement is an implementation issue as various traffic parameters could be used. Among the most used are the Buffer Occupancy, Link Utilization and Cell Loss Ratio (CLR). Process "B" involves simple arithmetical computations and is also implementation dependent. Process "D" represents a Protection Switching Process. Process "C" is explained below, using **FIG. 7** as an illustration.

FIG. 7 illustrates the main functions of one of the four processes involved in congestion prevention, namely the Selection of the Entity to be switched (Process "C" in **FIG. 6**).

The Process reads the real time statistics that present the current state of the network (in the node where the process is executed). If the onset of congestion is detected, the process checks if protection switching is allowed. Protection switching may not be desired if the traffic load on the protection path is such that traffic cannot be accommodated from the working path, in which case the human operator (network manager) sets a variable to inhibit protection switching. If Protection switching is allowed, the selection process starts. The selection process is implemented through a Function "Z." Function "Z" analyzes all entities (services or bundles of services) that cross the point of onset of congestion. Based on the priorities of the entities, and amount of carried traffic, only one entity is selected for protection switching. Then the protection switching is executed for the selected entity. If after a determined interval of time or observation period, the real time statistics still show the onset of

of traffic carrying entity. When the network load comes to a normal level for the observation period, the process is ended.

The priorities of the entities are established by the network operator. An example of how the priorities could be assigned is as follows:

Priority P0 (highest) - In this example, P0 is assigned to the services that are most sensitive to network impairments. The integrity of the cell stream for these services has to be guaranteed. Therefore a condition may be imposed by the network operator so that the services in this category should not be switched upon onset of congestion. These services impose conditions that may or may not be fulfilled during the protection switching process. As an example, Constant Bit Rate - CBR and real-time Variable Bit Rate - rtVBR impose restrictions both on the value of Cell Loss Ration (CLR) as well as the Cell Transfer Delay (CDT) or Cell Delay Variation (CDV). CLR, CDT and CDV are all QoS Parameters and reflect the sensitivity of the service to cell losses and to cell delays.

Priority P1 - In this example, P1 is assigned to the services that are less sensitive to network impairments, but do require some degree of QoS assurance. These services could be non real-time Variable Bit Rate - nrtVBR or Available Bit Rate - ABR. These services impose restrictions on the CLR, but are not concerned with delays in the network. Protection switching may be allowed for these services, if there is a guarantee that the number of lost cells during the protection switching will not exceed the maximum allowed CLR. In this case, only hitless (no cell loss) protection switching may be allowed.

Priority P2 (lowest) - In this example, P2 is assigned to the services that are not sensitive to cell losses nor delays. These services could be Unspecified Bit Rate - UBR services. These are the services that will be switched first in case of congestion onset.

The amount of carried traffic may or may not be specified. In case it is specified, it may be specified in various ways (Peak Cell Rate - PCR, Sustainable Cell Rate - SCR, Maximum Burst Size - MBS).

An illustration of the steps involved in selecting an entity for protection switching based on priority and amount of carried traffic is shown in **FIG. 8**.

is allowed for the respective priority, a search is performed in order to find entities that have that particular priority. If such entities are found, the selection process continues further for that priority of traffic. In case the amount of carried traffic is specified in some manner or another for the entities of that priority, the entity that is selected will be the one that carries the least amount of traffic. If the amount of traffic is not specified, then the entity selected is the first one to be found among all entities of the same priority in the database. If no entities carrying the desired priority are found, then the search will be initiated for the next higher priority. Before performing the search for entities of higher priority, the function must verify that the entities of that priority may be switched or not. In other words, the function must verify if the services of next higher priority allow protection switching or not, because of their sensitivity to losses or delays. In the case that protection switching is allowed for the higher priority and that there are entities of that higher priority, an entity of the higher priority will be selected. The process stops as soon as an entity is selected.

In the case that no entity can be selected (for example, if all entities have the same high priority and do not allow to be switched) protection switching cannot be performed. This is the reason why a careful planning of the network and services has to be performed in advance by the network operator.

FIG. 9 illustrates an example the operation of the congestion prevention mechanism for a given topology and for a given traffic load.

It is assumed that the traffic parameter selected as a Measure of Congestion is the link utilization. It is assumed as well that all links have the same capacity. Thus, if a link is utilized x%, the same amount of traffic on a different link will result in a link utilization of x% as well. It is also assumed that the alarm threshold is 65%, with a safety margin of 3%. This means that whenever the threshold of 65% utilization is reached and/or crossed for the observation period, onset of congestion state is declared and the congestion preventive mechanisms are triggered. The normal state is reached only after the link utilization has dropped below the alarm threshold with a value at least equal to the safety margin, for a complete observation period. In this case the link utilization has to be recorded at the most 62% for the

FIG. 9a shows the initial state of the network composed of five nodes, where the percentage values represent the link utilization. The protection switching is executed at the VPG level. Between node A and B a link utilization of 65% has been observed throughout the waiting period. After the selection process, VPG1 that carries traffic between A and C via B is selected and switched over to the protection path A to C via D.

FIG. 9b shows the state of the network after VPG1 has been switched. In average, VPG1 accounts for 5% of the link utilization. Since in this case the link utilization of link A-B dropped to 60% and this value has been recorded for a complete observation period, the normal state is declared and the selection/switching process is ended.

To perform the steps comprising the method of the present invention, the process can be implemented on a microprocessor or microcontroller platform, with access to the traffic parameters, and with communication access to the switching fabric. The technology can be implemented both in software and in hardware-software to be placed in existing and evolving network entities. In addition, the apparatus can be a stand-alone apparatus. The apparatus can be implemented as part of protection switching. The basic operation involves: buffer management; network management; dynamic diversion of the traffic; and integration to hitless, link and hard-node failure (apparatus failure).

The present invention can be used as part of commercial product such as a stand alone microprocessor-based board or as an ATM switch or VP cross-connect. The present invention can be easily integrated in protection switching apparatus that protects the network domains from node failure, link failure. The invention handles congestion as a soft-node failure and therefore, the node can quickly react to the traffic flow towards congestion and can prevent any loss of information or prevent any temporary delays to the traffic.

The implementation of a protection domain to provide the congestion prevention requires a modest spare bandwidth that can be used temporarily to prevent congestion occurrence as a soft-node failure. This does not significantly add to the cost of network operation, since networks are designed to have spare capacity for

The apparatus that uses the proposed invention will eliminate the need for significant over-provisioning of bandwidth to assure QoS at all times. Therefore, the present invention significantly reduces the cost of network operations and emergency repairs.

Having thus described the invention in detail, it is to be understood that the foregoing description is not intended to limit the spirit and scope thereof. What is desired to be protected by Letters Patent is set forth in the appended claims.

CLAIMS

What is claimed is:

1. A method for preventing congestion in an ATM network and insuring quality of service comprising:

providing closed loop congestion control methods utilizing feedback from the network to switch a fraction of the traffic from a primary path to secondary paths; and

at the same time, providing open loop congestion control methods by planning for additional bandwidth on the secondary paths.

2. The method of claim 1 wherein the step of providing closed loop congestion control methods includes monitoring traffic growth along a primary path.

3. The method of claim 2 wherein the step of providing open loop congestion control methods includes increasing resources.

4. The method of claim 3 wherein the step of providing open loop congestion control methods further includes decreasing traffic on the primary path by protection switching a fraction of the traffic to a secondary path.

5. A method for preventing congestion in an ATM network and insuring quality of service comprising the steps of:

monitoring traffic parameters on the network;

computing average growth of traffic on the network;

comparing the average traffic growth with pre-determined thresholds;

executing selective protection switching when the average traffic growth exceeds pre-determined thresholds, including:

selecting a traffic fraction to be switched; and

switching the selected traffic fraction to a secondary path;

continuing to monitor the traffic parameters; and

optionally returning to the original configuration of the network if the traffic parameters return to normal values for a selected time period.

6. The method of claim 5 wherein the step of selecting a traffic fraction to be switched comprises evaluating available bandwidth.

7. The method of claim 6 wherein the step of selecting a traffic fraction to be

virtual path groups.

8. The method of claim 7 wherein after the step of continuing to monitor the traffic parameters, if the traffic growth still exceeds predetermined levels, switching additional traffic to a secondary path.

9. A method of preventing congestion in an ATM network, and assuring quality of service, comprising:

sampling traffic parameters indicative of congestion;

computing average values for sampled traffic parameters;

storing average values in memory;

comparing average values to pre-set thresholds; and

initiating congestion prevention actions if average values exceed pre-set thresholds.

10. The method of claim 9 wherein the congestion prevention actions comprise selecting a fraction of traffic to be switched onto a protection path and switching the fraction of traffic onto the protection path.

11. The method of claim 9 wherein the fraction of traffic comprises a VC, VP or VPG.

12. The method of claim 10 further comprising selecting the traffic parameters to be sampled.

13. The method of claim 12 wherein the traffic parameters include buffer occupancy, link utilization or cell loss ratio.

14. The method of claim 12 wherein the pre-set thresholds relate to bandwidth.

15. The method of claim 12 wherein after switching the fraction of traffic to the protection path, traffic is again sampled, averaged, stored and compared, and if traffic still exceed pre-set thresholds, additional congestion prevention actions are initiated.

16. The method of claim 12 wherein the step of selecting a fraction of traffic to be switched comprises establishing priorities of entities and first selecting lowest priority entities for switching.

17. An apparatus for preventing congestion from occurring in an ATM network and assuming quality of service comprising:

measuring means for measuring traffic parameters in an ATM network;

means for switching of traffic from primary path to secondary paths prior to the onset of congestion.

18. The apparatus of claim 17 wherein the apparatus can be placed into existing networks.

19. The apparatus of claim 17 wherein the apparatus is a stand alone.

FIG. 1A

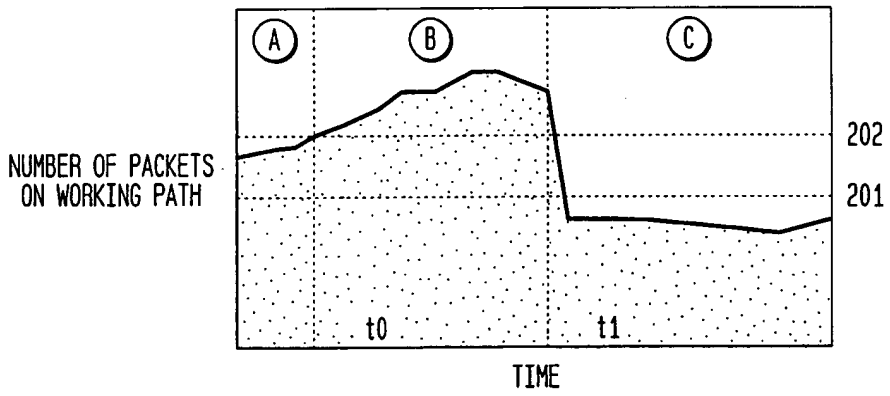

A
B
C
NUMBER OF PACKETS ON WORKING PATH
202
201
t0
t1
TIME

FIG. 1B

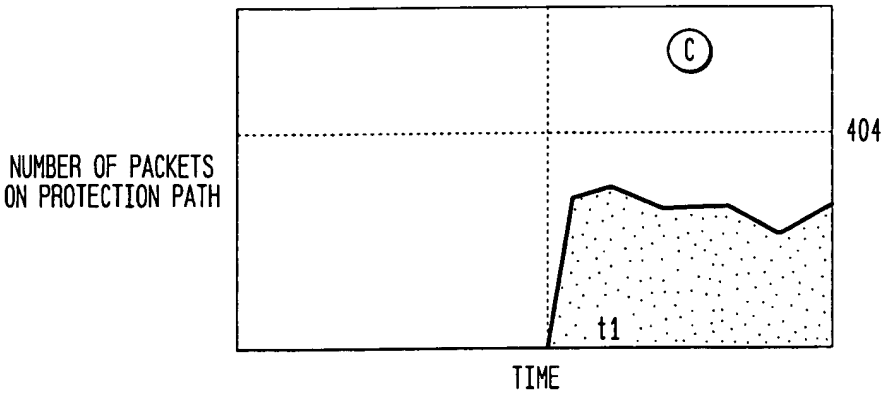

C
NUMBER OF PACKETS ON PROTECTION PATH
404
t1
TIME

FIG. 2

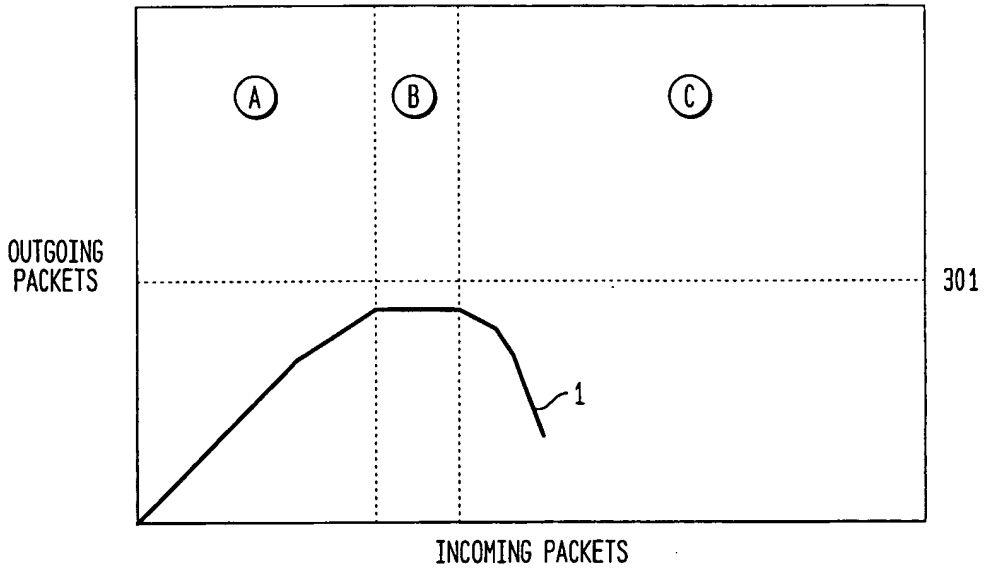

A
B
C
OUTGOING PACKETS
301
1
INCOMING PACKETS

FIG. 3

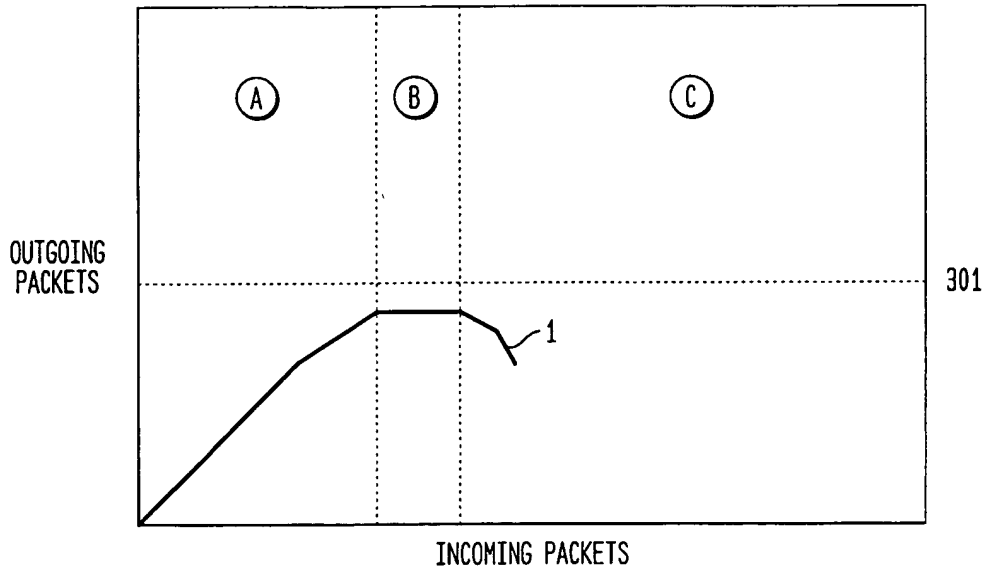

A
B
C
OUTGOING PACKETS
301
1
INCOMING PACKETS

FIG. 4

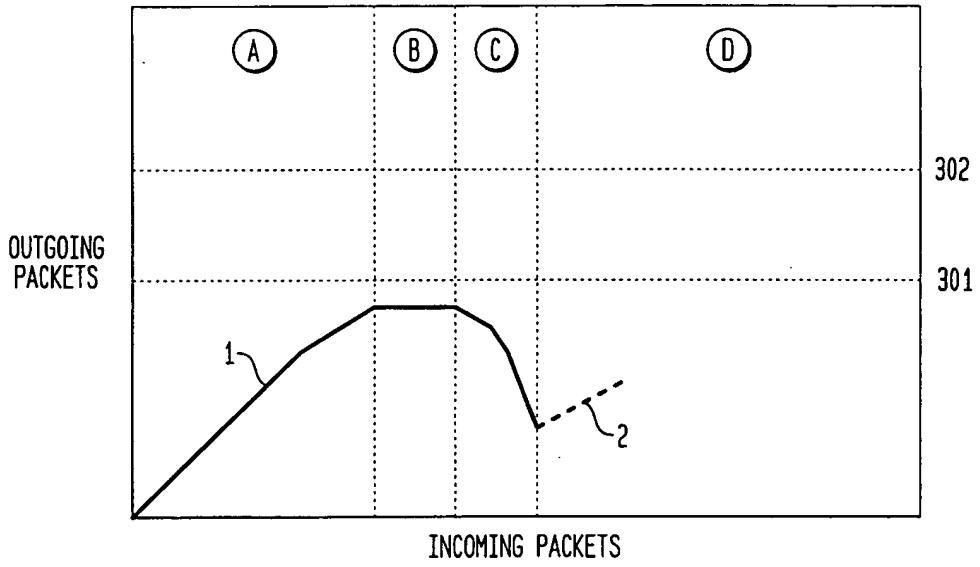

A
B
C
D
302
301
OUTGOING PACKETS
1
2
INCOMING PACKETS

FIG. 5

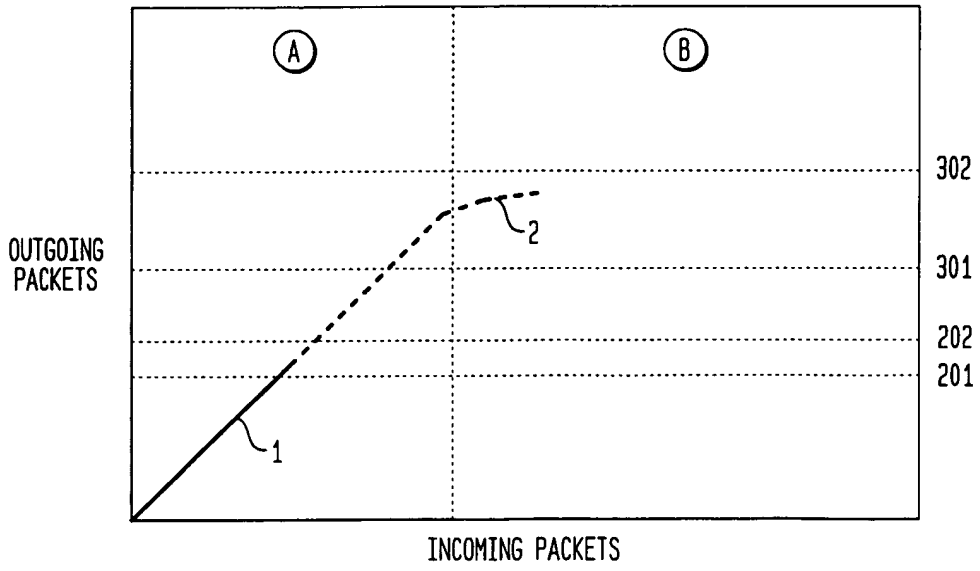
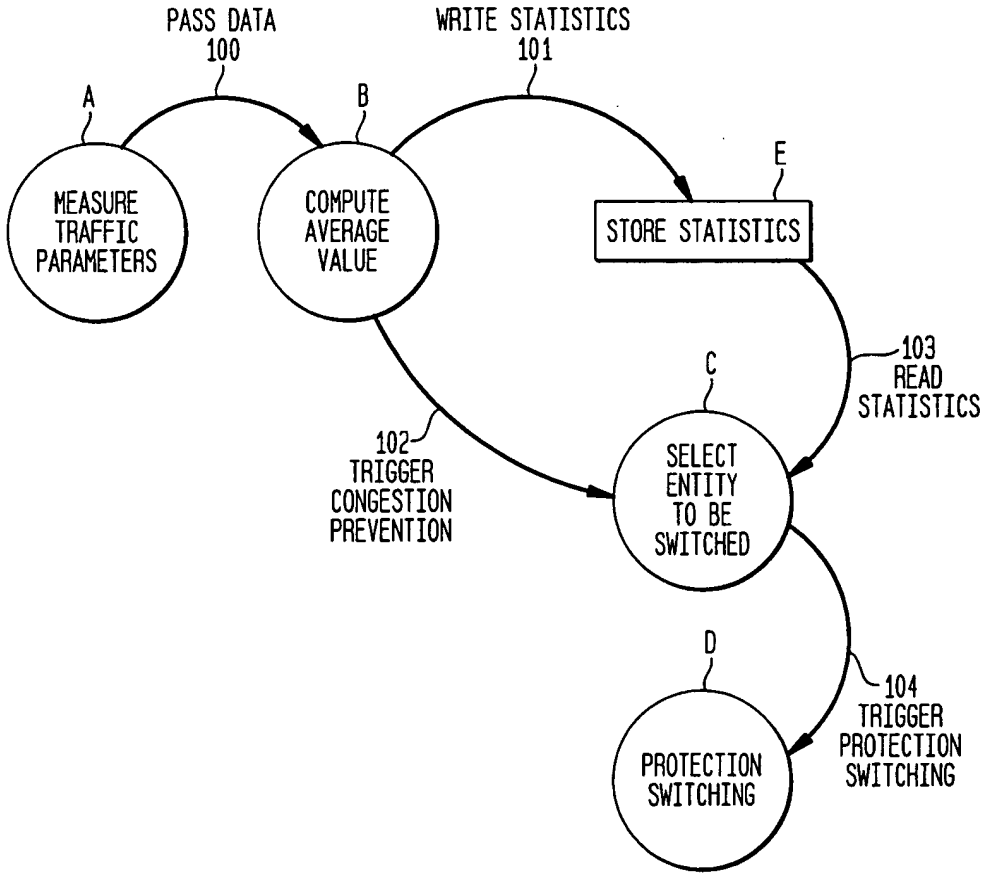

A
B
302
OUTGOING PACKETS
2
301
202
201
1
INCOMING PACKETS

FIG. 6


PASS DATA
100
WRITE STATISTICS
101
A
B
E
MEASURE TRAFFIC PARAMETERS
COMPUTE AVERAGE VALUE
STORE STATISTICS
103
READ STATISTICS
C
102
TRIGGER CONGESTION PREVENTION
SELECT ENTITY TO BE SWITCHED
D
104
TRIGGER PROTECTION SWITCHING
PROTECTION SWITCHING

5/7

FIG. 7

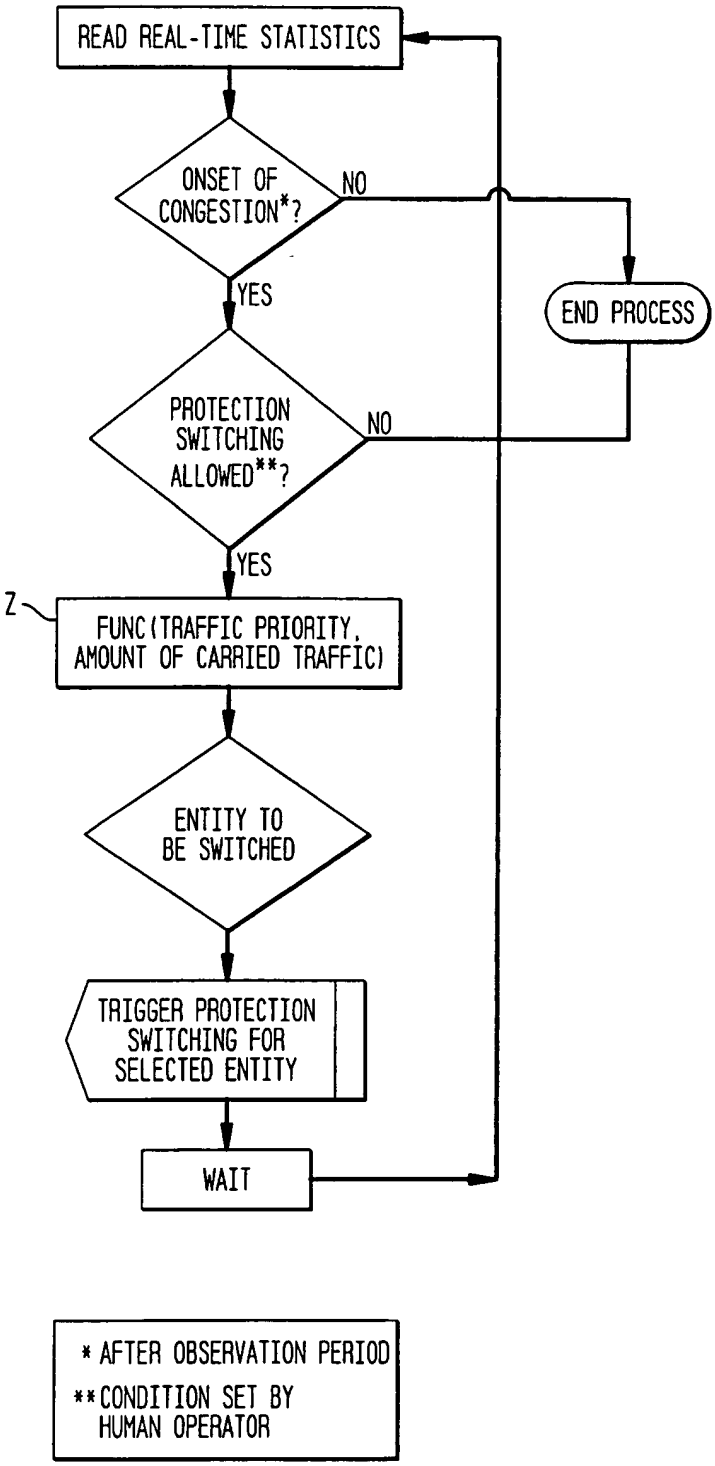

READ REAL-TIME STATISTICS
ONSET OF CONGESTION*?
NO
YES
END PROCESS
PROTECTION SWITCHING ALLOWED**?
NO
YES
Z
FUNC(TRAFFIC PRIORITY, AMOUNT OF CARRIED TRAFFIC)
ENTITY TO BE SWITCHED
TRIGGER PROTECTION SWITCHING FOR SELECTED ENTITY
WAIT
* AFTER OBSERVATION PERIOD
** CONDITION SET BY HUMAN OPERATOR

FIG. 8

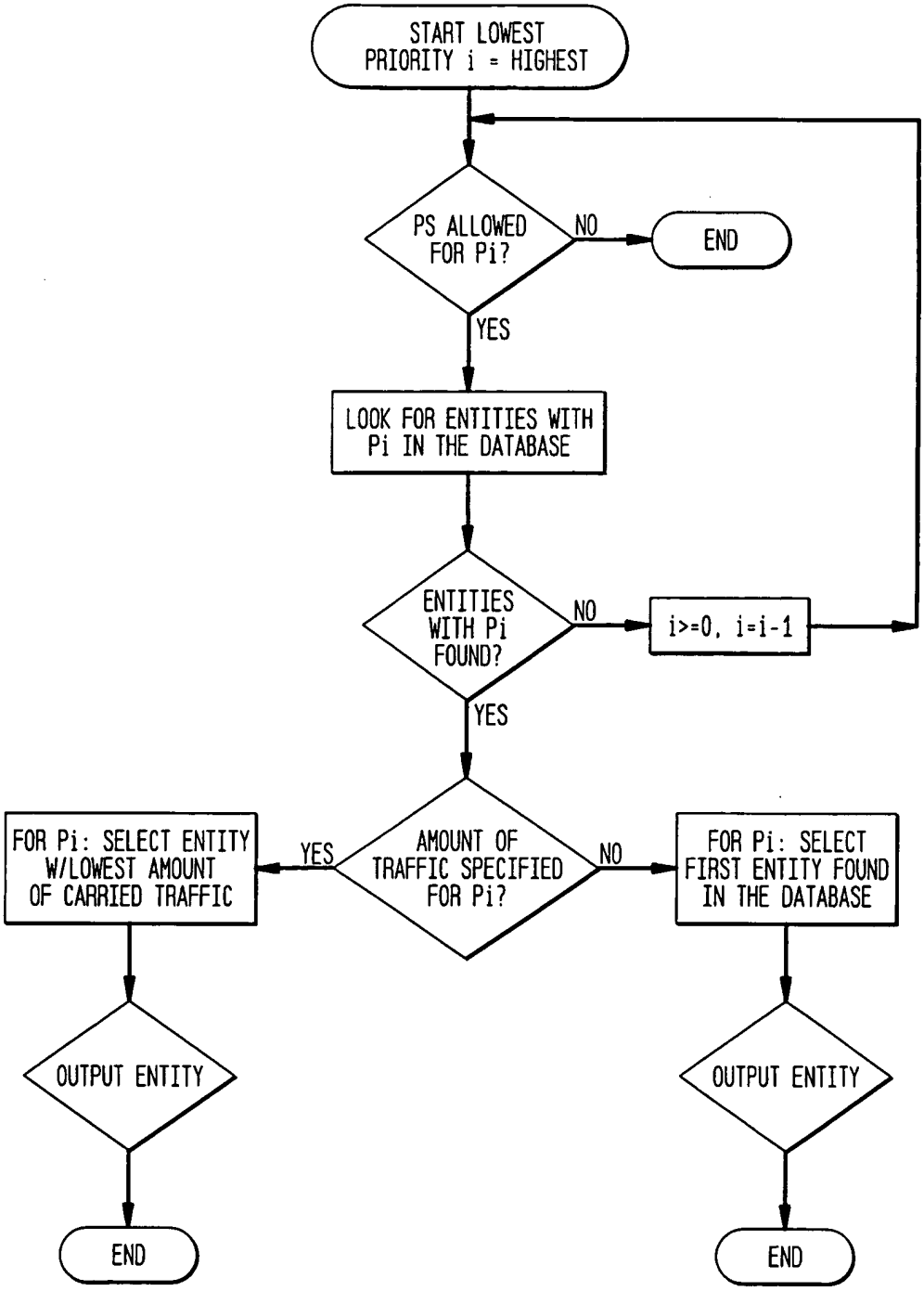

START LOWEST PRIORITY i = HIGHEST
PS ALLOWED FOR Pi?
NO
END
YES
LOOK FOR ENTITIES WITH Pi IN THE DATABASE
ENTITIES WITH Pi FOUND?
NO
i>=0, i=i-1
YES
AMOUNT OF TRAFFIC SPECIFIED FOR Pi?
YES
FOR Pi: SELECT ENTITY W/LOWEST AMOUNT OF CARRIED TRAFFIC
NO
FOR Pi: SELECT FIRST ENTITY FOUND IN THE DATABASE
OUTPUT ENTITY
OUTPUT ENTITY
END
END

FIG. 9A

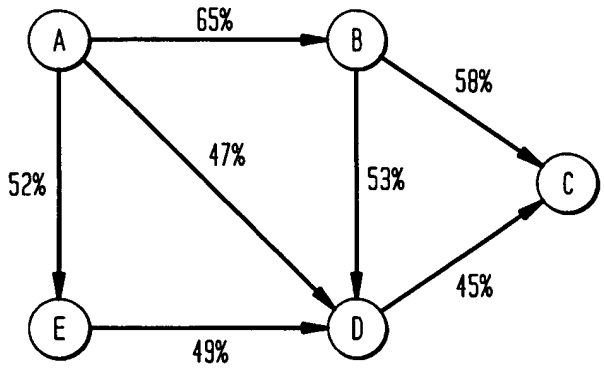


FIG. 9B